PX198

Expert report of Andrew Lewis-Pye

January 10, 2020

Securities and Exchange Commission v. Telegram Group Inc. and TON Issuer Inc

TABLE OF CONTENTS

I. Assignment

1. I have been retained by the law firm, SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP ("Counsel"), counsel for Telegram Group Inc. and TON Issuer Inc (the "Defendants") in the matter of *Securities and Exchange Commission v. Telegram Group Inc. and TON Issuer Inc*. Counsel has asked me to review the Expert Report of Maurice P. Herlihy submitted by the U.S. Securities and Exchange Commission ("SEC") on December 27, 2019 ("Herlihy Report") and other certain materials related to this case and to provide my expert opinion on certain claims made by the Herlihy Report. My opinions are stated below.

2. I have reviewed certain documents and publicly available information as described in Appendix A. All opinions are my own.

3. I am being compensated at $850 per hour in this matter. My compensation is not dependent on reaching certain opinions or the outcome of this litigation.

4. A list of documents relied upon in forming my opinions is provided in Appendix A.

5. I respectfully reserve the right to supplement, change, or modify my conclusions and summary of opinions, if additional information becomes available.

II. Qualifications

6. I am a Professor in the Department of Mathematics at the London School of Economics (UK). Prior to this I was a Royal Society University Research Fellow at the University of Leeds (UK) and at the London School of Economics, a Marie-Curie Fellow at the University of Siena (Italy) and an EPSRC Postdoctoral Fellow at the University of Leeds.

7. I have a B.A. in Mathematics from the University of Cambridge (UK), an MSc in Mathematics from the University of Manchester (UK), and a Ph.D. in Mathematics from the University of Leeds.

8. I have over 50 peer reviewed journal publications in various fields of algorithm/protocol design and analysis. For the last two years my research has focused on proof-of-stake protocols of the kind employed by the TON Blockchain. Since 2013 I have taught cryptography and cryptocurrencies to postgraduate students at the London School of Economics. Since 2018 I have been a consultant for Truebit, which is a scalability solution enabling the outsourcing of computation for blockchain smart contracts. My role at Truebit is to carry out a game theoretic analysis establishing long-term stable functionality for their scalability solution.

9. In summary, in the process of my own research on various blockchain consensus protocols, their scalability solutions and security features, as well as my industry consulting experience, I have reviewed and evaluated a large body of technical documentation for public ledgers and their underlying consensus protocols.

10. My Curriculum Vitae is attached as Appendix B to this report.

III. Summary of Opinions

11. In my view, the claims stated in the Herlihy Report are best categorised under two headings. First, the Herlihy Report claims that Telegram has failed to follow accepted norms for blockchain security analysis, in the sense that no peer-reviewed papers have thus far been produced establishing security of the system architecture prior to launch, and in the sense that the various versions of the TON white papers do not include mathematical analyses of security threats along

with proofs of correctness.[1] Second, the Herlihy Report states an opinion that certain key components are missing from the TON public code release and with regard to the collection of services surrounding the TON Blockchain.[2] I shall deal with these claims separately:

a. **The Alleged Accepted Norms for Blockchain Security Analysis.** With regard to the first claim of the Herlihy Report, i.e. the issue of security analysis performed prior to mainnet launch, the process followed by Telegram thus far is very much the norm for the industry. The strong implication of the Herlihy Report is that one should expect peer-reviewed papers establishing protocol security prior to launch, or at least that white papers should contain mathematical analyses of security threats along with proofs of correctness. In fact, for the most prominent and successful cryptocurrencies to date it has normally been the case that such analyses (where they exist) are developed over an extended period of time subsequent to launch, as a result of substantial back-and-forth interactions between academia and industry. I will consider the three blockchains Bitcoin, Ethereum and EOS for comparison. The first two of these are chosen because they are presently the two largest blockchains by market capitalisation,[3] while the example of EOS is chosen because its Initial-Coin-Offering ("ICO") raised more funds than any other to date, and because it shares certain significant commonalities with TON: Both use 'proof-of-stake' consensus protocols and are aimed at providing platforms for 'decentralised applications' ("Dapps"). The criteria outlined in the Herlihy Report were not fulfilled for any of these three examples at the time of launch.

[1] Herlihy Report, Paragraphs 16, 17, 35 and 36.
[2] Herlihy Report, Paragraphs 34 and 37.
[3] See: https://coinmarketcap.com/

b. **Alleged Missing TON Blockchain Code.** The second claim of the Herlihy Report states that "the public code release is missing a number of components critical to the TON Blockchain's functionality, including the core BFT consensus protocol, and the mechanisms by which validators are selected, rewarded, and punished for bad behavior."[4] In collaboration with a lead developer from the Truebit[5] development team, I have been able to verify that the code implementing the consensus algorithm for TON Blockchain has been available since September 7th 2019, and that the code controlling the distribution of validator awards, has also been available since the same date.[6] I shall examine further claims made by the Herlihy Report with respect to the allegedly missing TON Blockchain code in Section V below.

IV. The Accepted Norms for Blockchain Security Analysis Alleged in the Herlihy Report Do Not Exist.

12. In the remainder of Section IV, I shall be concerned with the examples of Bitcoin, Ethereum and EOS, and whether: (i) Peer-reviewed papers establishing protocol security were produced prior to launch, or (ii) White papers were produced prior to launch containing mathematical analyses of security threats along with proofs of correctness. Since the Herlihy Report claims that "no prudent investor or consumer would trust their assets to such a system without a thorough security analysis and audit",[7] however, it also seems appropriate to first consider the issue of security audits. In my view, obtaining a third-party audit prior to launching a project is neither standard practice nor required for market participation and user adoption. A review of

[4] Herlihy Report, Paragraph 34.
[5] See: https://truebit.io/
[6] While I was able to verify that this code has been made available, I did not audit the code.
[7] Herlihy Report, Paragraph 35.

seven prominent blockchain projects (*see* Appendix C) revealed that only one project, Algorand, had undergone an audit of their consensus protocol within two years of launching their mainnet. As far as I am aware, the other six are either yet to receive security audits at all, or received them well after their projects were launched, often having received hundreds of millions of dollars from purchasers in the interim.

13. The Bitcoin network was launched in January 2009. Prior to this, no peer-reviewed publications establishing security were produced. The Bitcoin white paper[8] is a well written document, but at nine pages, it contains a fairly minimal level of detail. An analysis of one particular form of double spending attack on the consensus protocol is given (to be secure a protocol must be secure against a wide range of attacks), but the analysis is simplistic and could not seriously be considered a proof of security, even against that one form of attack. A particular weakness of the analysis provided in the Bitcoin white paper, which is well understood by the academic community, is that it assumes a level of coordination between all 'honest' participants (i.e. those not engaged in an attack and behaving as the protocol asks them to) which may substantially fail to hold in reality, either by accident or due to manipulation by those engaged in an attack. Dealing with this weakness (in the analysis and in the protocol itself) was the main aim of the so called 'GHOST' protocol, introduced by Sompolinsky and Zohar in a paper of 2015.[9] It was not until a number of years after the launch of the Bitcoin network that anything regarding a convincing proof of security for the consensus protocol was produced — to my mind, perhaps the first serious analysis was

[8] The white paper is available at https://bitcoin.org/bitcoin.pdf.
[9] Sompolinsky Y., Zohar A. (2015) Secure High-Rate Transaction Processing in Bitcoin. In: Böhme R., Okamoto T. (eds) Financial Cryptography and Data Security. FC 2015. Lecture Notes in Computer Science, vol. 8975. Springer, Berlin, Heidelberg.

given by Garay et al. in a paper of 2015.[10] Even then, the proof of security rests on simplifying assumptions in terms of network connectivity and in terms of the ways in which users of the system will behave, which will not always hold in reality. The proof of Garay et al., for example, is naive from a game-theoretic perspective. In analysing an attack in which a certain user attempts to re-write which transactions are recorded in the blockchain, other users are assumed to follow the rules of the protocol simply because they are 'honest' rather than because they have explicit incentive to carry out such action. Such game-theoretic issues, and the issue of 'selfish mining' in particular,[11] have been shown to be potentially problematic for the Bitcoin protocol. Establishing a rigorous proof of security for the Bitcoin consensus protocol is thus still an ongoing and substantial project for researchers in academia and industry.

14. In addition to the underlying consensus protocol, Bitcoin makes use of a 'smart contract language', which is just the formal language allowing users to specify how transactions should be executed. Although less sophisticated than that used by Ethereum, this smart contract language should reasonably have been considered a significant potential point of vulnerability at time of launch. The smart contract language was not described in the Bitcoin white paper, and was not described or analysed in any peer-reviewed papers prior to network launch. No code audit was publicised prior to launch, and at least one update has been required in order to deal with a major security flaw.[12]

[10] Garay J., Kiayias A., Leonardos N. (2015) The Bitcoin Backbone Protocol: Analysis and Applications. In: Oswald E., Fischlin M. (eds) Advances in Cryptology - EUROCRYPT 2015. Lecture Notes in Computer Science, vol. 9057. Springer, Berlin, Heidelberg.
[11] Ittay Eyal and Emin Gun Sirer. Majority is not enough: Bitcoin mining is vulnerable. Communications of the ACM, 61(7):95-102, 2018.
[12] See: "Vulnerability Summary for CVE-2010-5139". National Vulnerability Database. June 8, 2012 and https://nvd.nist.gov/vuln/detail/CVE-2010-5139https://nvd.nist.gov/vuln/detail/CVE-2010-5139

15. By December 2014, and prior to the point at which anything approaching a serious mathematical proof of security had been produced, Bitcoin had a market capitalisation in excess of $4 billion and was widely traded and utilised in transactions on the blockchain.[13]

16. The Ethereum Network was launched in July 2015. The underlying consensus protocol used was (and remains) a variant of that used by Bitcoin — the white paper[14] describes a variant of the Bitcoin consensus protocol which uses elements of the GHOST protocol of Sompolinsky and Zohar, but which also has points of deviation with the protocol described in their paper. I am not aware of any peer-reviewed paper which deals specifically with Ethereum's variant of the GHOST protocol, and its white paper does not include a proof of security.

17. The big innovation of Ethereum separating it from Bitcoin, was the inclusion of a much more sophisticated smart contract language, named 'Solidity'. While Solidity was not described in detail in the white paper, the lead developer, Christian Reitwiessner, started creating a list of features and making them available online as of January 2015, initially on the Ethereum wiki,[15] then at github.com/ethereum/aleth and then on solidity.readthedocs.io/. No proof of security for this smart contract language was attempted in the white paper or supporting documentation, and as far as I am aware no peer-reviewed paper was produced prior to launch attempting any such analysis. Since the rise to prominence of the Ethereum blockchain, the issue of formal verification for smart contract languages (i.e. the establishing of formal mechanisms which can be used to check that smart contracts will behave as intended) and for the Solidity language in particular, has attracted significant interest from the verification community (in computer science, 'formal veri-

[13] See: https://coinmarketcap.com/currencies/bitcoin/historical-data/?start=20141210&end=20200109
[14] Available at https://github.com/ethereum/wiki/wiki/White-Paper
[15] See: https://github.com/ethereum/wiki/wiki/Solidity-Features/1372fa4d3cf487114c623e24c03233e2adf37c66

fication' means proving or disproving that algorithms will perform as intended). Again, the establishing of appropriate frameworks for analysis is an ongoing and substantial project for researchers in academia and industry.

18. While the question of security for Ethereum is a substantial matter of ongoing concern,[16] it presently has a market capitalisation in excess of approximately $15 billion.[17] Zeppelin, a security audit firm for blockchain systems, conducted a security audit on the Solidity compiler and language for potential security vulnerabilities in the general design and architecture that may compromise the compiled code.[18] The security audit was co-sponsored by the Ethereum Foundation and Augur with a grant of $430,000.[19] As far as I am aware, this was the first such audit carried out and was published on November 1, 2018, more than three years after the Ethereum public launch. By the end of October 2018, Ethereum already had a market capitalisation in excess of $20 billion and was widely traded and utilised in transactions on the blockchain.[20]

19. In common with Bitcoin, the existing consensus protocol used by Ethereum is what is referred to as a 'proof-of-work' protocol (meaning that the integrity of the blockchain is ensured by certain users of the network carrying out extensive, and otherwise useless, computations). Two of the most substantial differences between Ethereum and the TON Blockchain are:

(i) The TON Blockchain employs a 'proof-of-stake' consensus protocol. Proof-of-stake is an alternative to proof-of-work, which has attracted significant interest because it wastes less energy, and also has significant potential security and scalability benefits.

[16] See for example, the paper of Chen et al. available at https://arxiv.org/pdf/1908.04507.pdf, or the paper of Atzei et al. available at https://eprint.iacr.org/2016/1007.pdf
[17] See: https://coinmarketcap.com/
[18] See: https://docs.google.com/document/d/1PZBSCBWBwd6AqWCgXqLnw8FNQ4HRurP5usrXuKuU0a0/edit
[19] See: https://blog.ethereum.org/2018/05/02/announcing-may-2018-cohort-ef-grants/
[20] See: https://coinmarketcap.com/currencies/ethereum/historical-data/?start=20180801&end=20200109

(ii) The TON Blockchain is 'sharded', which means that the protocol runs multiple blockchains and allows for interactions between those chains. The motivation for such an implementation is to increase transaction rates, i.e. the number of transactions that can be processed per second.

20. It is therefore significant to note that the Ethereum Foundation has repeatedly stated its intention to move to a proof-of-stake protocol,[21] and also to move over to the use of a sharded blockchain protocol.[22] The reasoning behind this is straightforward. As well as wasting vastly less energy, it is the asserted opinion of Vitalik Buterin (co-founder of Ethereum) that (properly implemented) proof-of-stake protocols potentially offer significant security benefits over proof-of-work protocols as well as reduced centralisation risks.[23] Sharding is part of the Ethereum Foundation's approach to dealing with the need for increased transaction rates, and the present understanding is that proof-of-stake protocols may be more amenable to successful implementations of sharding.

21. Similar to TON, EOS makes use of a proof-of-stake consensus protocol. The proof-of-stake consensus protocol used by EOS is a form of 'Delegated-Proof-of-Stake' ("DPoS"). As far as I am aware, there are no peer reviewed papers establishing security for the DPoS protocol employed by EOS. In EOS white papers[24] a high-level description of the DPoS protocol is given, but no attempt is made at a mathematical analysis of security.

[21] See: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ or https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51
[22] See: https://github.com/ethereum/wiki/wiki/Sharding-roadmap
[23] See: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ
[24] See: https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md and https://whitepaperdatabase.com/eos-whitepaper/

22. Both EOSIO (the EOS protocol) and TON make use of a special set of users, called 'block producers' in EOSIO and 'validators' in TON, whose job is to build and maintain the security of the blockchain. Concerns have been raised over centralisation pressures for EOS,[25] in part because it is designed to be limited to only 21 block producers at any one time.[26] By contrast, the TON white paper asserts that the intention is to begin with a set of 100 validators, possibly increasing to 1000 over time. In this regard, I note the Herlihy Report's observation that 36 validators were detected on the TON testnet, well more than the limit of 21 block producers for EOS.[27] All else being equal, this larger set of validators (as opposed to 21 block producers) will decrease centralisation risks and (while the details of the protocol are significant here) will also tend to decrease vulnerability to Denial-of-Service attacks.[28]

23. While no mathematical proof of security has yet been provided, EOS has had the largest ICO to date, raising in excess of $4 billion and is widely traded and utilised in transactions on the blockchain.[29] As far as I am aware no professional third party audit of the kind that Zeppelin performed for Ethereum (as referred to in Paragraph 18 above) has been performed for EOS prior to launch.

24. In summary, my review establishes that the most successful public blockchains in existence today did not provide peer-reviewed publications establishing protocol security prior to launch, did not produce white papers containing mathematical analyses of security threats along with proofs of correctness, and did not commission third-party security audits prior to launch. The

[25] See for example https://www.coindesk.com/everyones-worst-fears-about-eos-are-proving-true
[26] Grigg, Ian, "EOS: An Introduction". July 5, 2017, p. 3. See: https://iang.org/papers/EOS_An_Introduction-BLACK-EDITION.pdf
[27] Herlihy Report, Paragraph 33.
[28] A denial-of-service attack is a malicious attempt to overwhelm an online service and render it unusable.
[29] See: https://www.cnbc.com/2018/05/31/a-blockchain-start-up-just-raised-4-billion-without-a-live-product.html

accepted norms for blockchain security analysis alleged in the Herlihy report simply do not exist, and the process followed by Telegram thus far is very much the norm for the public blockchain industry.

V. Allegedly Missing TON Blockchain Code.

25. The Herlihy Report claims that "the public code release is missing a number of components critical to the TON Blockchain's functionality, including the core BFT consensus protocol, and the mechanisms by which validators are selected, rewarded, and punished for bad behavior."[30] In collaboration with a lead developer from the Truebit development team, I was able to verify that the implementation of the consensus algorithm has been available since September 7th 2019 at https://github.com/ton-blockchain/ton/tree/master/catchain and https://github.com/ton-blockchain/ton/tree/master/validator-session, and that the code controlling the distribution of validator awards has also been available since the same date at https://github.com/ton-blockchain/ton/blob/master/crypto/smartcont/elector-code.fc.[31]

26. I take the claim that the code implementing the core BFT consensus protocol is missing, to be the most significant of the objections regarding missing code made in the Herlihy Report. Three other statements which are made regarding missing code are: (i) Herlihy was unable to find the code controlling the creation of new workchains (activities on the TON Blockchain are split among a 'masterchain' and a number of 'workchains'), (ii) He was unable to find the code for rewarding fishermen (fishermen are a type of user that attempts to gain rewards by establishing the existence of invalid blocks), and (iii) He was also unable to find code executing the 'vertical

[30] Herlihy Report, Paragraph 34.
[31] While I was able to verify that this code has been made available, I did not audit the code.

blockchain' functionality, which is a mechanism for quickly updating the blockchain in the case that errors are found.[32] However, these components are not a core part of the blockchain functionality being required for the launch of the mainnet.

27. With respect to the creation of new workchains, the Herlihy Report asserts that the code could not be located on the testnet, but also that "it is natural that the 'testnet' release would not permit such creation . . . ."[33] I am informed by counsel on behalf of Telegram that the code required for the creation of new workchains has in fact been available at the GitHub repository. My review of the TON White Paper also indicates that only the initial workchain, so called "Workchain Zero", is used to transfer the TON cryptocurrency Grams, and that most applications are likely to require only this workchain. This makes the code responsible for the creation of new workchains non-critical for a launch or operation of a functional TON blockchain.

28. Assuming the code for rewarding fishermen has not been made available, the use of fishermen is not common (and might be particular to the TON Blockchain at this point). This is an additional layer of security, which can be added to the core protocol at a later date, by the TON development team or other users of the network.

29. The use of vertical blockchains is not standard or necessary for blockchain functionality (as far as I am aware this idea was also unique to the TON Blockchain). I am informed by counsel that, during testing by the TON development team, it was determined that the use of vertical blockchains decreased the stability of the network and has been replaced by a concept of "legal forks." So, the code implementing vertical blockchain functionality is not there, because it

[32] Herlihy Report, Paragraphs 29-32.
[33] Herlihy Report, Paragraph 29.

has been replaced by another apparatus aimed at achieving the same task, and which has been made publicly available.

* * * * * * * * *

Respectfully submitted,
Dated: January 10, 2020

Andrew Lewis-Pye

Appendix A: Documents Relied Upon

Case-Related Documents

Expert Report of Maurice P. Herlihy (Dec. 27, 2019)

Other Documents

Bitcoin: A Peer-to-Peer Electronic Cash System (Oct. 31, 2018)

Ethereum – A Next-Generation Smart Contract and Decentralized Application Platform (Jun. 17, 2019)

EOS – An Introduction (Jul. 5, 2017)

EOS.IO Technical White Paper v2 (Mar. 16, 2018)

Academic Publications

Atzei, Nicola, Massimo Bartoletti, and Tiziana Cimoli. "A Survey of Attacks on Ethereum Smart Contracts." in Principles of Security and Trust, (pp. 164–186), Springer, Berlin, Heidelberg, 2017.

Chen, Huashan, Marcus Pendleton, Laurent Nijilla, and Shouhuai Xu. "A Survey on Ethereum Systems Security: Vulnerabilities, Attacks and Defenses." arXiv preprint arXiv:1908.04507, 2019.

Sompolinsky, Yonatan, and Aviv Zohar. Secure High-Rate Transaction Processing in Bitcoin. In International Conference on Financial Cryptography and Data Security (pp. 507-527). Springer, Berlin, Heidelberg, Jul. 16, 2015.

Garay, Juan, Aggelos Kiayias, and Nikos Leaonardos. "The Bitcoin Backbone Protocol: Analysis and Applications." In Advances in Cryptology – EUROCRYPT 2015 – 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 281-310). Springer, Berlin, Heidelberg, Apr. 14, 2015.

Eyal, I., & Sirer, E. G. (2018). Majority is not enough: Bitcoin mining is vulnerable. Communications of the ACM, 61(7), 95-102, Nov. 15, 2013.

Appendix B – Curriculum Vitae

PROF. ANDREW E.M. LEWIS-PYE

Home address
141d Southwood Lane,
Highgate,
London, UK, N6 5TA.
(+44) 7850 681662
andy@lewis-pye.com, a.lewis7@lse.ac.uk
homepage: www.lewis-pye.com

University address
Department of Mathematics, LSE,
Houghton Street,
London, UK, WC2A 2AE
(+44) 203 4862955.

Education

Undergraduate: 1st in Mathematics, University of Cambridge.

MSc in Mathematical Logic, (one year course) University of Manchester.

PhD, Computability theory, University of Leeds, under the supervision of Barry Cooper.

I completed the PhD in two years (actually one year, but university rules stipulate a minimum of two years), and reached the final shortlist of three for the Sacks prize, awarded each year for the best PhD in mathematical logic worldwide.

Previous positions and awards

Options trader for Mako-Global Derivates.
Prior to my PhD, ten months during the period 2000-2001.

EPSRC Postdoctoral Fellowship in Mathematics.
Hosted at the University of Leeds, 2003-2005.

A maximum of ten given each year to young researchers in mathematics nationwide.

Marie-Curie Fellowship.
Hosted at the University of Siena, 2005-2007. Host contact: Andrea Sorbi.

Royal Society University Research Fellowship.
Hosted at the University of Leeds, 2007-2013, 2013-2015 at the LSE.

These are eight year fellowships. An average of one or two are given to pure mathematicians each year, with a total of twenty five to thirty throughout science as a whole.

Department of Mathematics, London School of Economics.
2013–present. Associate Professor since 2015, (full) Professor since 2019.

Papers

Papers are listed in roughly reverse chronological order. All names on papers appear in alphabetical order.

1) *The idemetric property: when most distances are (almost) the same*, with Barmpalias, Huang, Li, Li, Pan, and Roughgarden, Proceedings of the Royal Society A, vol 475, Issue 2222, 2019.

2) *Compression of data streams down to their information content*, with Barmpalias, IEEE Transactions on Information Theory, vol 65, Issue 7, 2019.

3) *Monotonous betting strategies in warped casinos*, with Barmpalias and Nan Fang, to appear in Information and Computation.

4) *Limits of the Kucera-Gacs coding method*, with Barmpalias, to appear in Proceedings of SEALS 2017.

5) *The search for natural definability in the Turing degrees*, Computability, 1–47, 2017.

6) *Establishing social cooperation: the roles of hubs and community structure*, with Cooper, Li, Pang and Yong, to appear in Network Science.

7) *A note on the differences of computably enumerable reals*, with Barmpalias, Proceedings of the International Symposium on Computability and Complexity (in honour of Rod Downey's 60th birthday), Lecture Notes in Computer Science 10010 Springer, 2017.

8) *Optimal redundancy in computations from random oracles*, with Barmpalias, Journal of Computer and System Sciences, 92, 1–8, 2018.

9) *Differences of halting probabilities*, with Barmpalias, Journal of Computer and System Sciences, 89, 349–360, 2017

10) *Optimal asymptotic bounds on the oracle use in computations from Chaitin's Omega*, with Barmpalias and Fang, Journal of Computer and System Sciences, 82, 1283-1299, 2016.

11) *Computing halting probabilities from other halting probabilities*, with Barmpalias, Theoretical Computer Science, 660, 16-22, 2017.

12) *Minority population in the one dimensional Schelling model of segregation*, with Barmpalias and Elwes, Journal of Statistical Physics 173(5), 1408–1458, 2018.

13) *Pointed computations and Martin-Löf randomness*, with Barmpalias and Li, Computability, vol 7, no 2-3, 171–177, 2018.

14) *Lower bounds on redundancy in computations from random oracles*, with Barmpalias and Teutsch, Information and Computation, 251, 287-300, 2016.

15) *Sex versus Asex: the role of variance conversion*, with Montalbán, Theoretical Population Biology, 114, Jan 2017.

16) *From randomness to order: Schelling segregation in two or three dimensions*, with Barmpalias and Elwes, Journal of Statistical Physics 164 (6), 1460-1487, 2016.

17) *Tipping points in Schelling segregation*, with Barmpalias and Elwes, Journal of Statistical Physics 158 (4), 806–852, 2015.

18) *The complexity of computable categoricity*, with Downey, Katch, Lempp, Montalbán and Turetsky, Advances in Mathematics, 268, 423–466, 2015.

19) *C.e. degrees and the meet property*, with Durrant, Ng and Riley, Proceedings of the American Mathematical Society 144, 1735-1744, 2016.

20) *The information content of typical reals*, with Barmpalias, Turing's Ideas - Their Significance and Impact, G. Sommaruga, T. Strahm (eds.), Basel, Birkhuser / Springer Basel, 2015.

21) *Digital Morhphogenesis via Schelling segregation*, with Barmpalias and Elwes, FOCS 2014, 55th Annual IEEE Symposium on Foundations of Computer Science, Oct. 18-21, Philadelphia, 156–165. Journal version, Nonlinearity 31, 1593-1638, 2018.

22) *The typical Turing degree*, with Day and Barmpalias, Proceedings of the London Mathematical Society, 109 (1), 1–39, 2014.

23) *Diagonally non-computable functions and bi-immunity*, with Carl Jockusch, Journal of Symbolic Logic 78 (3), 977-988, 2013.

24) *Measure and cupping in the Turing degrees*, with George Barmpalias, Proceedings of the American Mathematical Society, Volume 140, Number 10, 3607-3622, 2012.

25) *Chaitin's halting probability and the compression of strings using oracles*, with George Barmpalias, Proceedings of the Royal Society A, 467, 2912-2926, 2011.

26) *Analogues of Chaitin's* Ω *in the c.e. sets*, with Barmpalias, Hölz and Merkle, Information Processing Letters, 113(5-6):171-178, 2013.

27) *Extensions of embeddings below computably enumerable degrees*, with Rod Downey, Noam Greenberg and Antonio Montalbán, Transactions of the American Mathematical Society 365, 2977-3018, 2013.

28) *A note on the join property*, Proceedings of the American Mathematical Society, Volume 140, Number 2, February 2012, 707714.

29) *Topological aspects of the Medvedev Lattice*, with Richard Shore and Andrea Sorbi, Archive for Mathematical Logic 50, 319-340, 2011.

30) *Empty intervals in the enumeration degrees*, with Thomas Kent and Andrea Sorbi, Annals of Pure and Applied Logic. Volume 163, Issue 5, 567-574, 2012.

31) *Joining up to the generalized high degrees*, with Phil Ellison, Proceedings of the American Mathematical Society, 138, 2949-2960, 2010.

32) *On the degree spectrum of a* Π^0_1 *class*, with Thomas Kent, Transactions of the American Mathematical Society, 362, 5283-5319, 2010.

33) *The importance of* Π^0_1 *classes in effective randomness*, with George Barmpalias and Ken Meng Ng, Journal of Symbolic Logic, Volume 75, Number 1, 2010.

34) *The first order theories of the Medvedev and Muchnik lattices*, with Andrea Sorbi and Andre Nies, Lecture Notes in Computer Science 5635, 324 - 331.

35) *On a question of Slaman and Groszek*, Proceedings of the American Mathematical Society, 136, 3663-3668, 2008.

36) *A fixed point free minimal degree*, with Masahiro Kumabe, Journal of the London Mathematical Society 80 (3): 785-797, 2009.

37) Π^0_1 *classes, LR degrees and Turing degrees*, with George Barmpalias and Frank Stephan, Annals of Pure and Applied Logic, 156, 21-38, 2008.

38) *A random degree with strong minimal cover*, Bulletin of the London Mathematical Society 39 (5), 848-856, 2007.

39) Π^0_1 *classes, strong minimal covers and hyperimmune-free degrees*, Bulletin of the London Mathematical Society, 39 (6): 892-910, 2007.

40) *Working with the LR degrees*, with George Barmpalias and Mariya Soskova, Theory and Applications of Models of Computation: 4th International Conference TAMC 2007, Shanghai China, Proceedings, Springer Lecture Notes in Computer Science, LNCS 4484, 89-99, 2007.

41) *Lowness, Randomness and Degrees*, with George Barmpalias and Mariya Soskova, Journal of Symbolic Logic 73, issue 2, 559-577, 2008.

42) *A weakly 2-random which is not* GL_1, with Antonio Montalbán and Andre Nies, Lecture Notes in Computer Science vol 4497.

43) *Strong minimal covers and a question of Yates: the story so far*, Proceedings of the Logic Colloquium 2006, Lecture Notes in Logic 32.

44) *The ibT degrees of c.e. sets are not dense*, with George Barmpalias, Annals of Pure and Applied Logic, volume 141, Issues1-2, 2006.

45) *The jump classes of minimal covers*, Logical Approaches to Computational Barriers, Second Conference on Computability in Europe, CiE 2006, Lecture Notes in Computer Science, 307-318.

46) *A partial solution to a question of Sacks*, New Computational Paradigms, proceedings of CiE 2005, Lecture Notes in Computer Science 3526, 275-286.

47) *Randomness and the linear degrees of computability*, with George Barmpalias, Annals of Pure and Applied Logic, volume 145, issue 3, 252-257, 2007.

48) *A single minimal complement for the c.e. degrees*, Transactions of the American Mathematical Society 359, 5817-5865, 2007.

49) *The hypersimple-free wtt degrees are dense in the c.e. wtt degrees*, with George Barmpalias, Notre Dame Journal of Formal Logic, volume 47 Isuue 3, 2006.

50) *Random reals and Lipschitz continuity*, with George Barmpalias, Mathematical Structures in Computer Science, volume 16, issue 5, 2006.

51) *A c.e. real that cannot be sw computed by any* Ω *number*, with George Barmpalias, Notre Dame Journal of Formal Logic, vol 47 (2), 197-209, 2006.

52) *The minimal complementation property above* $0'$, Mathematical Logic Quarterly, 51 (5), 470-492, 2005.

53) *Properly* Σ_2 *minimal degrees and* $0''$ *complementation*, with Barry Cooper and Yue Yang, Mathematical Logic Quarterly, 51, 274-276, 2005.

54) *Finite cupping sets*, Archive for Mathematical Logic, 43, 845-858, 2004.

55) *Minimal complements for degrees below* $0'$, Journal of Symbolic Logic, 69 (4), 937-966, 2004.

Invited Talks (a selection)

- Plenary talk, TAMC, Beijing, 2004.
- Special session talk, CiE, Amsterdam 2005.
- Special session talk TAMC, Kunming, 2005.
- Plenary talk, British Logic Colloquium 2005.
- Plenary talk, Logic Colloquium, Nijmegen, 2006.
- Special session talk, CiE, Swansea 2006.
- Plenary talk, Russian Algebra and Logic meeting, Kazan 2006.
- Special session talk, ASL meeting, Gainsville 2007.
- Special session talk, CiE, Siena, 2007.
- Plenary talk, ASL meeting, Irvine 2008.
- Plenary talk, The Computability Workshop, Sofia 2009.
- Special session talk, AMS meeting, Notre Dame 2010.
- Invited series of lectures, Notre Dame 2011.
- Plenary talk, Midwest computability meeting, Chicago 2011.
- Plenary talk, Computational Prospects of Infinity, Recursion Theory, Singapore 2011.
- Oberwolfach workshop on computability, 2012.
- Dagstul workshop on computability, 2012.
- Newton Institute, Cambridge 2012.
- Special session talk, The Incomputable, Chicheley Hall 2012.
- Plenary talk, CCR, Cambridge 2012.
- Plenary talk, Colloquium Logicum 2012.
- Plenary talk, MALOA, Luminy 2013.
- Special session talk, CiE, Budapest, 2014.
- Special session talk, Latin-American Symposium on Mathematical Logic in Buenos Aires, 2014.
- FOCS 2014.
- Tutorial, Computability days, Paris, 2015.
- Plenary talk, British Colloquium for Theoretical Computer Science, 2015.
- MLAC, Tehran 2016.
- SEALS, Gainesville, 2017.
- Panhellenic Logic Symposium 2017.

Other academic activity

- Programme Committee member Crypto-Economics Security Conference, Berkeley 2019.
- Programme Committee member, Workshop on Trusted Smart Contracts 2020.
- Admissions, MSc in Financial Mathematics, LSE, 2015-2017.
- Seminar on Combinatorics, Games and Optimisation, joint organiser, 2016.
- Research Committee, Department of Mathematics, LSE, 2014–present.
- Athena Swan committee, Department of Mathematics, LSE, 2016–2017.
- USSC (Undergraduate Studies Sub-Committee) Member, 2017–present.
- Co-chair of the programme committee for CCR 2015 in Heidelberg (Computability, Complexity and Randomness).
- Programme committee member for TAMC (Theory and Applications of Models of Computation).
- Member of the organising committee for the Computability in Europe meeting in Siena, 2007.
- MALOA training committee member.
- Chair of the organising committee for the Computability Workshop, 2010 (Azores).
- Chair of the steering committee for the annual Computability Workshop.
- I have refereed for many journals, including Advances in Mathematics, the Proceedings and the Journal of the London Mathematical Society, the Proceedings of the American Mathematical Society, the Journal of Symbolic Logic, the Journal of Mathematical Logic, the Annals of Pure and Applied Logic, the Archive for Mathematical Logic, Theoretical Population Biology, Games and Economic Behaviour, Proceedings of the Royal Society A, the Journal of Statistical Physics and others.
- Reviewer for Zentralblatt MATH.
- With Dugald Macpherson and Peter Schuster, I organised the British Logic Colloquium 2013 in Leeds.
- FWF Austrian Science Fund proposal reviewer.
- Grant proposal reviewer for EPSRC.

Appendix C - Observed Security Audits and Certifications on Selected Projects

Entity	Current Market Cap[1]	Reported Launch Date of Platform	Observed Public 3rd Party Audit and Certification[2]
Ethereum	$15B	July 30, 2015[3]	July 12, 2018[4] and November 1, 2018[5]
Stellar	$928M	July 2014[6]	None identified
Tether	$4.6B	February 25, 2015[7]	August 2017[8] and January 3, 2018[9]
EOS	$2.6B	June 2018[10]	None identified
Filecoin	Not listed	Testnet launched December 11, 2019; Mainnet estimated March 2020[11]	None identified
Algorand	$115M	June 19, 2019[12]	June 18, 2019[13]
Hedera Hashgraph	$20M	September 16, 2019[14]	None identified

[1] Market cap is as of January 9, 2020 from https://coinmarketcap.com/all/views/all/
[2] Represents identified instances where an entity engaged an independent third-party to audit or publicly certify its code. These were identified via online searches of each entity's websites, if available, and searches of companies which appear to provide these audits, including OneZeppelin, Runtime Verification Inc., Quantstamp, and others.
[3] Refers to "Frontier", the described "official public mainnet launch" of the Ethereum project, see: https://consensys.net/blog/blockchain-explained/a-short-history-of-ethereum/ and https://blog.ethereum.org/2015/07/30/ethereum-launches/
[4] See: https://github.com/runtimeverification/verified-smart-contracts/blob/master/casper/protocol-verification.md
[5] See: https://docs.google.com/document/d/1PZBSCBWBwd6AqWCgXqLnw8FNQ4HRurP5usrXuKuU0a0/edit
[6] See: https://fortune.com/2014/07/31/stripe-launches-bitcoin-challenger-gives-it-away-for-free/
[7] Refers to when Tether was first trading, see: https://bitcoinmagazine.com/articles/warning-signs-timeline-tether-and-bitfinex-events
[8] Date inferred from certain dates identified in the report, see: https://stableset.com/audits/tether_audit_v1/tether_audit_v1.pdf
[9] See: https://blog.openzeppelin.com/tether-token-audit-438d561a380/
[10] See: https://block.one/news/eosio-1-0-release/
[11] See: https://filecoin.io/blog/update-2019-q2-q3/#1-launches-testnet-on-dec-11-mainnet-in-2020-q1
[12] See: https://algorand.foundation/algorand-foundation-announces-first-auction
[13] See: https://runtimeverification.com/blog/formally-verifying-algorand-reinforcing-a-chain-of-steel-modeling-and-safety/
[14] See: https://hbarprice.com/hbar-coin-release/